Access 5 Project Office
NASA
P.O. Box 273
Edwards, CA 93523 USA
661-276-2440
661-276-3880 FAX
www.access5.aero

COVER SHEET

Access 5 Project Deliverable

Deliverable Number: IMP006

Title: *Common Operating Picture – UAV Security Study*

Filename: *IMP006_Common_Operating_Picture-UAV_Security_Study_v1_FINAL.doc*

Abstract:

This initial communication security study is a top-level assessment of basic security issues related to the operation of UAVs in the NAS. Security considerations will include information relating to the use of ICAO Aeronautical Telecommunications Network (ATN) protocols and applications identifying their maturity, as well as the use of IPV4 and a version of mobile IPV6. The purpose of this assessment is to provide an initial analysis of the security implications of introducing UAVs into the NAS.

Status:

SEIT-Approved

Limitations on use:

This document represents thoughts and ideas of the Implementation and Infrastructure work package team. It has been reviewed and approved by the SEIT but has not been reviewed or approved by the Project Office as official Access 5 Project recommendations on this subject.

Common Operating Picture
UAV Security Study

October 29, 2004

The following document was prepared by a collaborative team through the noted work package. This was a funded effort under the Access 5 Project.

Table of Contents

Executive Summary

The present architecture for the operation of UAVs consists of proprietary UAV and AVCS components that communicate over largely unprotected spectrum using free text messaging for Pilot to UAV ATC communications, command and control, and flight termination. It is imperative that security mechanisms for protection from denial of service and jamming, authentication, encryption, and non-repudiation be in place for this line of communication before UAVs can be introduced to the NAS. As a part of this report, we have also identified the importance of having flight termination capabilities as well as the need to make sure non-repudiation techniques are present for this function.

It is assumed that one way for the UAV's pilot to communicate with the FAA is by use of a "bent pipe". When the UAV pilot wants to initiate communication with ATC controllers, communication is established between the pilot and UAV and the UAV and ATC controller. Other than the risk of being eavesdropped there is no real threat to the avionics systems in the UAV with this approach, when properly designed.

ICAO currently functions using the OSI protocol stack on the ATN network. This system has been deployed for a while and has thus had some time to mature. However, with the TCP/IP protocol stack gaining immense popularity and the need to interoperate with a growing number of new applications that only support TCP/IP, the ATN is being forced to transition towards TCP/IP. Work is currently under way for this effort and the ATN is looking at both IPv4 and IPv6, with the latter protocol having a better chance of being selected due to its attractive security features and its ability to work in a mobile environment.

It is our recommendation that if UAVs wind up embracing IP technology, vigorous security testing be done to make sure that known security vulnerabilities with IPv4 are mitigated and unknown security vulnerabilities with IPv6 are identified.

Finally, in order to deploy UAVs in the NAS, the airships must meet all FAA rules and regulations imposed by manned aircraft. A formal security assessment will need to be done on the finalized design of the UAV communication systems and airship, when this occurs.

1 Introduction

This initial communication security study is a top-level assessment of basic security issues related to the operation of UAVs in the NAS. Security considerations will include information relating to the use of ICAO Aeronautical Telecommunications Network (ATN) protocols and applications identifying their maturity, as well as the use of IPV4 and a version of mobile IPV6. The purpose of this assessment is to provide an initial analysis of the security implications of introducing UAVs into the NAS.

1.1 Objectives

The objectives of the NASA UAV Initial Communications Security Study are to:

1. Provide a high level overview of the envisioned communication architecture required to support UAV Operations.
    i. In the near-term, gather and document information on the current and envisioned communications architecture required for UAVs to operate in the NAS.
    ii. Identify the current and/or envisioned voice and data communications architecture required to support routine UAV operations.
2. Review ICAO progress on moving from an OSI based protocol suite to IP based protocols and their maturity to support UAV operations.
3. Identify security holes in A/G and G/G infrastructure.
4. Perform a preliminary security assessment of the voice and data architectures.
5. Review the possible concerns and the attendant mitigation activities using the FAA Security Certification and Authorization Package (SCAP) Template.
6. As part of this review assess each protocol suites potential security holes as they apply to this application and propose standard mitigations.
7. Assess ATN and IP protocols for maturity of design and security.

1.2 Discoveries and Assumptions

As we gathered the data, the study team made the following discoveries and assumptions:

1. No overall communication architecture is presently available for UAVs.
2. No common communication architecture for UAV command and control is currently available for security assessment.
3. Each UAV manufacturer has its own command and control, payload, and flight termination communications architecture.
4. Each portion of the communication architecture may be bundled or have varying degrees of separation depending on the manufacturer's design criteria.
5. Each portion of the communication architecture uses the same protocol types (such as all OSI, all TCP/IP, etc...)
6. UAV's use radio frequencies that are not assigned for the specific purpose of UAV operations.
7. Some UAV manufacturers use radio frequencies in unregulated wireless communication bands, e.g., 900 MHz, 2.4 GHz, and 5 GHz.
8. Many UAVs transmit command & control information using clear text.
9. UAV Pilots will communicate with Air Traffic Control using one of two methods:
    a. dial-up/leased line into an ATC facility
    b. the aircraft C and C link to provide Pilot to UAV comm. and then cross-link that voice transmission to the appropriate ATC UHF or VHF channel.
10. If CPDLC is used for pilot to controller communication, it is assumed that it is the ICAO Aeronautical Telecommunications Network (ATN) Protocol Implementation Compliance Statements (PICS) for Open Systems Interconnection (OSI) protocol that will be used.
11. Line-of-Site (LOS) and Satellite is assumed to be the communication path between controller and UAV.
12. Both LOS and Satellite communication assumed to be using same protocol suite at the Network Layer (layer 3 of the OSI model) since both should provide the same functionality (Physical and Data link may vary, but the security assessment will be mainly focused on Network Layer and above).
13. UAV Pilot is assumed to coordinate with FAA via ground communications (such as phone line)
    a. The current infrastructure cannot accommodate phone-line communication to ATC controllers (phone #s not published).
    b. To support the current NAS architecture, the UAV must act as the media

converter between pilot and controller (having secure voice or VoIP technology from Pilot to UAV and then convert that to UHF or VHF communication from UAV to the Air Traffic Controller.)

14. The UAV Pilot may be in a fixed or mobile facility or vehicle.
    a. When they are in mobile vehicles, cellular phone technology may be used in order to communicate with the controllers through the PSTN. A future assessment of cellular phone security needs to be included if this is the case.
15. There may be more than one UAV pilot in one or more locations.
16. UAVs cannot use the Traffic Alert & Collision Avoidance System (TCAS) for autonomous movement, per FAA aircraft certification and flight standards. However, this should be pursued as possibly being allowed as a "last resort" option.
17. When the Command and Control link becomes inoperable the UAV is assumed to be intelligent, allowing for independent decisive measures during loss of communication with UAV controller.
18. If the UAV is capable of autonomous decision making when the Command and Control link is inoperative, the function will most likely be considered Critical for the safe execution of the mission earning the most rigorous design and development standards for airworthiness and operational approval.
19. To meet Part 91 "see and avoid" requirements in both VFR and IFR conditions, the UAV may provide the pilot "see and avoid". There are several possible ways: payload surveillance systems, flight only surveillance systems, Automatic Dependent Surveillance –Broadcast and rebroadcast of ADS-B.
20. To operate as 14 CFR 91 aircraft, it is assumed that the aircraft equipment will meet the requirements of 14 CFR 21 using FAA Advisory Circulars and Technical Standards Orders as a means of showing compliance with the regulations. These documents may refer to various RTCA, International Civil Aviation Organization, Society of Automotive Engineers and other documents.
21. For rotorcraft UAVs other parts of the FAR may be applicable e.g. 14 CFR 27.
22. Assume ATN will have successfully converted to IP or have mechanisms to carry OSI over IP or vice versa by 2010. (Based on feedback from the FAA Air Traffic Operation Planning Communication System Engineering staff).
23. Safety is part of security, but will not be part of this assessment. Safety concerns include guarding against unintentional mishaps that result from design or procedural issue.

2 Overview of UAVs

UAVs come in fixed wing and rotorcraft configurations. They come in many sizes and have varying degrees of complexity in their design and operation. The most sophisticated UAVs have the capability to takeoff and land like conventional manned aircraft.

Presently, UAVs are restricted in how they are permitted to operate in positive controlled airspace. Flights occur infrequently and require weeks of planning and coordination with the Federal Aviation Administration (FAA). When those flights occur they must start and end in Military Operations Areas (MOAs). Prior to entering civilian, positively controlled airspace the UAV must be at flight level above where civilian traffic operates (e.g. FL410). It is the desire of the operators to be able to operate under 14 CFR 91 (aka the Federal Aviation Regulations) like manned aircraft that operate in the NAS. Government and Commercial operators of Unmanned Aerial Vehicles want to be able to operate in the National Airspace System like manned aircraft.

To that end, NASA, other government agencies, and the vendor consortium known as UNITE have united together to develop technology, procedures, training, etc. that will allow UAVs to operate in the NAS. That project is known as Access 5. The FAA participates in Access 5 as an advisor only. Several FAA organizations are key participants in Access 5, e.g., Aircraft Certification, Flight Standards, Spectrum Management, Air Traffic, etc. As part of Access 5 research work, NASA's Langley Research Center was asked to examine the security considerations involved in operating a UAV in the NAS.

3 Communication Architecture

The following sections identify the communication architectures of operations of UAVs in the NAS. Figure 3 provides a picture of the communication between the pilot and UAV.

3.1 Envisioned Communication Architecture

UAVs typically have aircraft and ground based control components. Among different UAV vendors there is no common architecture or functional allocation of requirements between aircraft and ground sites. Access 5 documentation and other research indicates that the current UAV communications system architecture can be viewed as four separate parts some of which may use the same communications path(s) and RF Links. These parts are categorized into:

1. Command and Control (C^2) (Pilot-to-Aircraft, with telemetry from aircraft-to-pilot)
2. Air Traffic Control (Pilot-to-FAA)
3. Payload (mission traffic, such as surveillance information)
4. Flight Termination (onboard or remote emergency termination)

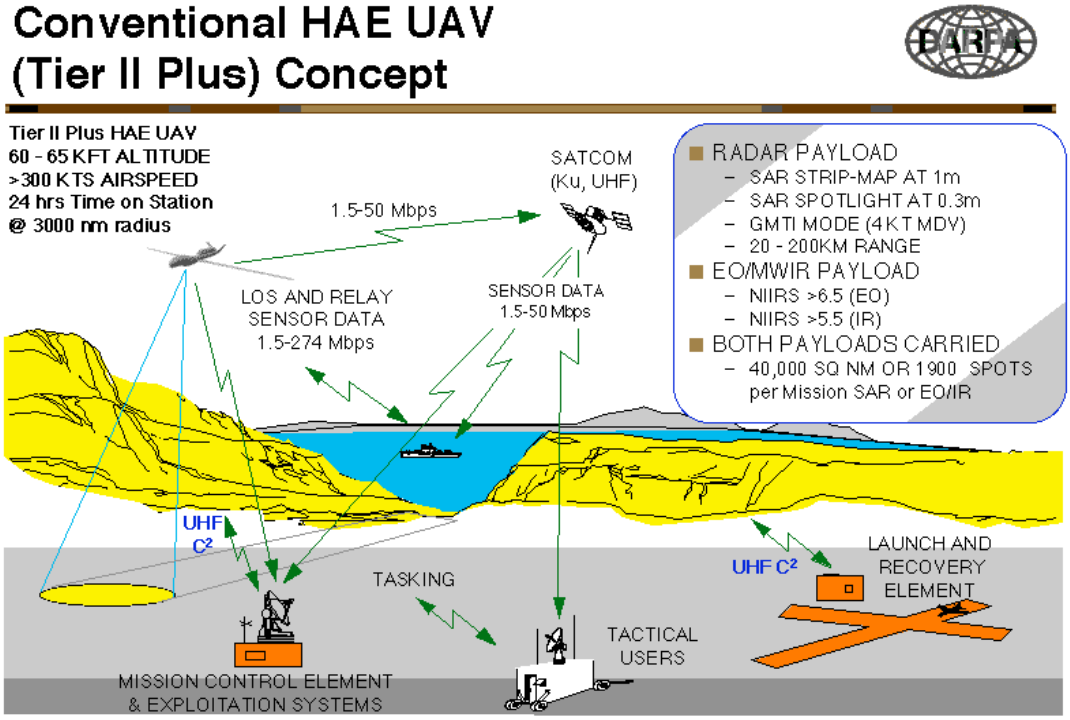

Figure 1 Conventional HAE UAV (Tier II Plus) Concept

http://www.fas.org/irp/program/collect/global_hawk.htm

Each function may operate in separate pieces of the spectrum or be combined together. The only ITU-T/FCC licensed spectrum for these 4 areas is the ATC UHF and VHF bands. Some UAVs use spectrum reserved for military use when in a MOA. However, once the UAV leaves the MOA, C^2, Payload, and Flight Terminal together or separately may suffer from intentional (jamming) or unintentional interference (operating in an unregulated band e.g., 900 MHz, 2.4 MHz, & 5 GHz.)

3.1.1 Command and Control (C^2)

The Command and Control (C^2) portion is the functionality that provides aircraft situational awareness to the pilot of the aircraft's behavior and the ability to control its movements. The RF path for the aircraft may have line of sight and satellite components. The aircraft may start the flight using the LOS path and switch to satellite when out of LOS range (over the horizon). UAVs can operate at 900 MHz, 2.4 GHz, etc. Some military UAVs such as Predator or Globalhawk operate in bands assigned to the U.S. Department of Defense but not necessarily reserved for UAV operations. Based on input from the FAA Spectrum Management office, it appears that no UAVs use RF paths with protected service volumes specifically licensed for the purpose of UAV flight operations. Discussions with SAIC UAV experts indicate that UAVs use proprietary C^2 free text, human readable protocols.

The data link between the AVCS and the UAV can be considered to be the most critical part of the UAV operations. The components of this include the uplink that carries the critical C^2 traffic and/or voice and the downlink that is mainly responsible for carrying the payload traffic such as imagery/voice and may include a separate channel for obtaining management info from the UAV as well as acknowledgement traffic for various commands issued. For the purpose of this study, we assume that all these channels are all part of a single data stream that needs to be secured entirely.

Interviews and online research suggest that currently the C^2 link as well as the payload downlink are not encrypted. Compression techniques, based on a custom sequence, are used for some of the communications. Spread spectrum and frequency hopping have been identified as either being used or planned for use to some extent (not fully identified, partially due to proprietary and confidential reasons). Even with compression techniques, spread spectrum, and frequency hopping though, the payload message can be intercepted and decoded. There is also no authentication being used. Since there is no authentication,

the communication can be manipulated (modification of data or taking over control of the C^2) link.

Security is paramount for the link between the AVCS and UAV. It is recommended that cryptographic technology be used for encrypting the data channel as well as authenticating the end devices. If IPv4 or IPv6 is used as the network layer protocol for this traffic, then IP Security (IPsec) technology can be utilized to provide authentication as well as encryption for privacy.

It is important to make sure that the latest in encryption algorithms are employed as well. Earlier encryption methods such as DES are now known to have flaws. AES is the current widely deployed encryption algorithm that provides most security by enabling use of keys as big as 256 bits (DES used 56-bit keys).

One of the concerns with implementing this technology for UAV to AVCS communication is the hand-off process. If there's a disruption in the link during the handoff (a hard handoff vs a soft handoff) there is a chance that any established IPsec tunnel can break. If this is the case, the tunnel would have to be setup again and the system could become vulnerable at that point where an attacker might try to break into the data connection. Handoff between pilots should use a "make before break" strategy, ensuring communication with the UAV is not lost between transitions.

Another concern has to do with how IP addresses are going to be used within the UAVs. This should be a topic for further research since no information is available right now. The concern has to do with how the IP addresses are going to be assigned to the UAV. If the IP addresses are hard-coded into the UAVs, and the UAV gets handed over to another AVCS, that AVCS might be in a totally different IP subnet. For the UAV to keep communicating, it would have to utilize the mobile IP technology in order to keep communicating with the same IP address. There are security issues identified with using mobile IP that would have to be taken into consideration.

Finally, if the UAVs plan on using multicasting to broadcast the payload data to be shared by several AVCSs, then IPsec cannot be used directly with multicast traffic, mainly due to the fact that key management is difficult with the way multicast protocol works. A workaround to this problem would be to create a GRE tunnel or something similar to tunnel the multicast traffic through or use layer 2 encryption devices at either

end to perform the encryption of frames in the data link layer. This solution can be used for securing all the data paths involved with UAV communications but it is not scalable as two encryption boxes are need to support each peer-to-peer connection and as it would not scale for multiple peer-to-peer connections that are envisioned.

3.1.2 Air Traffic Control

During flight, pilots communicate with the FAA's Enroute and Approach Control (ARTCC/TRACON) facilities. The UAV's pilot will need to perform this function. The following discusses the possible ways this communication may occur, since there is nothing currently in place.

The communication between pilot and FAA uses the allocated frequency for that airspace. This is primarily voice communication using VHF or UHF frequencies allocated to the specific EnRoute Center or Approach Control. This communication path is not secure, and presents the same security concerns as other plain-text communications.

It is assumed that one way for the UAV's pilot to communicate with the FAA is by use of a "bent pipe". When the UAV pilot wants to initiate communication with ATC controllers, communication is established between the pilot and UAV and the UAV and ATC controller. The uplink frequency and downlink frequency would be converted at the UAV. The same communication would occur when the ATC needed to contact the UAV pilot. The positive aspect is that since the current voice system is all analog, there need not be any security filtering at the interface of the radios onboard the UAVs and the interface that is responsible for carrying that traffic through the system in the UAV down to the pilot. The analog voice channel cannot be used to launch any attack on the data network system present on the UAV, since this system would not be connected to the command systems of the UAV. Ghost controllers and ghost pilots in the ATC voice system are usually eliminated because real ATC controllers and pilots can easily identify the ghost's lack of AT language usage knowledge and professionalism.

Another way to perform the communication requirement between the UAV pilot and FAA and between the FAA and UAV pilot is to use a land line PSTN line. This would be accomplished by the UAV pilot having access to a dedicated UAV controller, or hunt access line to controllers at each location needing to be contacted. The controllers would need access numbers for the UAV pilots. Secure telephones could be used for this

solution. This will become a very complex option to manage and use as the number of UAVs increases.

3.1.3 Payload

The payload is the mission traffic sent from the UAV to a receiving site. This communication path can be air-to-ground (such as UAV to ground station), or air-to-air (such as UAV to air station). The data in this payload may be surveillance (such as ground or air data) or other mission of the UAV data.

The communication medium for payload data may be the same medium used for the command and control and flight termination data. If the data are co-mingled a security assessment of the risks and vulnerabilities will need to be done. If the payload data is not as protected as the flight termination, a payload application compromise could gain access to flight termination functionality.

The payload communication is primarily a one-way transmission of data (from UAV to receiving site). However, communications to the systems that provide this transmission are still required. The payload may or may not be sensitive information that needs to be protected. The payload systems may or may not impact UAV flight operations.

3.1.4 Flight Termination

Flight termination deals with the need to identify a means to terminate a UAV's mission in the event control is lost and the autonomous operations has failed. There are different ways to accomplish flight termination generally in two categories, from a remote signal or from an onboard scenario. A remote signal can be sent from a ground or air station. The air station could position itself next to the UAV and send a close distance signal. The signal can tell the UAV to "return to base, fly into ground, or flat spin and fall". It is recommend that the strategy chosen uses 14 CFR 91 rules for loss of ATC communication as a guide.

3.2 ICAO Progress

The following sections review the International Civil Aviation Organization (ICAO) ATN progress, the progress on moving from an OSI based protocol suite to IP based protocols, and their maturity of ATN to support UAV operations.

3.2.1 ATN Background

The Aeronautical Telecommunications Network (ATN) has been developed by the International Civil Aviation Organization (ICAO) as a strategy for integrating Air/Ground and Ground/Ground data communications networks into a global internet serving Air Traffic Control and Aeronautical Operational Communications.

The ATN fully supports mobile communications over a wide variety of mobile communications networks including AMSS, VDL, and Mode S. With the ATN, it is possible for a ground system to communicate with airborne avionics in any part of the world. The listed RF media are the only ones licensed for Air Traffic use for safety of flight communications, ITU-T, and ICAO.

The ATN is an internetwork built on top of existing networks through the use of routers as gateways between those networks. It is designed based on the ISO OSI Reference Model and associated ISO OSI standardized data communications protocols. When the ATN was designed, the TCP/IP protocol had not gained widespread popularity. ISO Open Systems Interconnection (OSI) model was encouraged to be used in the architecture to provide interoperability between other ATN links.

ICAO has also developed a set of Air Traffic Control applications that are ATN compliant. These applications Controller Pilot Data Link Communications (CPDLC), Flight Information Services (FIS), Automatic Dependent Surveillance (ADS) (the addressable one), Aeronautical Message Handling Service (carry AFTN traffic over the ATN), and Context Management. CPDLC has the entire lexicon of ATC phraseology contained in ICAO ANNEX 2 and is used in place of voice communications. CPDLC is encoded using ASN.1 and reduces the message size from that of free text to something much smaller. It also has the advantage of making the message machine processable without any pre-processing. Flight Information Services provides weather data such as digital ATIS and NOTAMS. FIS is air initiated and sets up agreements with ground applications about which weather messages and what type of updates can be requested.

The standard Abstract Syntax Notation No. 1 (ASN.1) is used to specify messages in their abstract syntax. The ASN.1 Packed Encoding Rules (PER) is typically used for Air/Ground user data in order to give efficient communications.

All end systems and routers on ATN support the ISO 8473 Connectionless Network

Protocol (CLNP). This is the ATN Internet Protocol (IP) and provides a common format for all packets exchanged by the ATN. The Network Service Access Point address for the aircraft uses the aircraft 24-bit ID as part of the address. In the United States, with the exception of military aircraft, the 24-bit ID maps is unique and maps to the aircraft tail number.

ATN uses IDRP as its routing protocol on the backbone. IDRP is a distant vector routing protocol. Routers advertise only the routes that they want to advertise. It's a policy driven protocol such that routes are only advertised when permitted by the effective routing policy, and contain only the information the routing policy allows to be advertised.

Each aircraft is considered to be in a domain of its own and has an ATN router that is a Boundary Intermediate System (BIS). The ground system may be composed of one or more routing domains each with its own ATN router BIS. All paths between the aircraft and ground end systems are known by all of the BIS. Ground based A/G routers do not necessarily have to be connected to the RF medium. They simply must have knowledge of the path. Also, each RF path may be in a different routing domain so long as the Ground A/G router advertises a viable path to the end system. As an aircraft transits the airspace it may change routing domains to which it is attached as well as end systems and applications. The aircraft and the ground systems can choose among the available RF paths using quality of service parameters. The network takes advantage of the protocol suite's self-healing abilities at the network layer and in reality can accept any subnetwork that presents a compliant interface and meets throughput and latency requirements.

A/G routing is initiated by either air or ground BIS when a new RF path is discovered at the data link layer. Through a mobile routing service initiation event, air and ground routers exchange reachability information including reachable end systems, Quality of Service (QoS) parameters, and Routing Policy. Once the routers and reachable end have been advertised to the network, application initiation may begin. At this point the aircraft does not have ATC ground system application addresses.

Each aircraft is considered to be in a domain of its own and has an ATN router that is a BIS. The ground system may be composed of one or more routing domains each with its own ATN router BIS. All paths between the aircraft and ground end systems are known by all of the BIS. Ground based A/G routers do not necessarily have to be connected to

the RF medium. They simply must have knowledge of the path. Also, each RF path may be in a different routing domain so long as the Ground A/G router advertises a viable path to the end system. As an aircraft transits the airspace it may change routing domains to which it is attached as well as end systems and applications. The aircraft and the ground systems can choose among the available RF paths using quality of service parameters. The network takes advantage of the protocol suite's self-healing abilities at the network layer and in reality can accept any subnetwork that presents a compliant interface and meets through put and latency requirements.

A/G routing is initiated by either air or ground BIS when a new RF path is discovered at the data link layer. Through a mobile routing service initiation event, air and ground routers exchange reachability information including reachable end systems, Quality of Service parameters, and Routing Policy. Once the routers and reachable end have been advertised to the network, application initiation may begin. At this point the aircraft does not have ATC ground system application addresses.

A/G application initiation may only be started by the aircraft using an application called Context Management (CM). CM is a means by which aircraft do not have to carry specific addresses for each ATC service provider. This is necessary because cockpit automation systems have limited computing resources and the ATC service provider list and applications availability list can be quite lengthy as compared to the onboard resources. CM is initiated by a log-on command that may be human entered or by machine upload from the Airline Operations Center. In version 2 of the CM application, a secure logon may be requested. The logon is conveyed to the ground CM application in the appropriate domain. The logon is checked for validity. If the logon is from a valid aircraft, then the addresses of the applications and their end systems are sent back to the aircraft CM. The crew may then logon to the available applications. In the United States an active, valid flight plan with positive Flight ID matching is required as a minimum before the ground CM application will return end system and application addresses. If there is no active, valid flight plan a pilot must air file his flight plan before gaining access application and end system information.

Once the application and end system addresses are received on the aircraft, it is free to start one or more application associations (e.g. CPDLC). Any instruction for the aircraft to deviate from its present course requires pilot approval before the Flight Management System can execute the change. Most messages have a series of possible acceptable

responses. Where a response is needed, the response is displayed to the Air Traffic Controller in the flight data block for that aircraft. Controller CPDLC eligibility is controlled by which sector is responsible for the aircraft. Controller eligibility is displayed in the flight data block also. Pilots may also make requests of controllers. Depending on the implementation in the ATC automation system, the system may compose a suggested response for the controller.

Addressable ADS can only be initiated by the ATC system. The reporting agreements are set by the ground system. There is also a limited pilot interface that permits the ADS update rate to go to 1 position report per second should an in-flight emergency be declared.

As aircraft transition ATC facilities the next facility applications and addresses are provided to the next ATC facility by the current ATC facility so that the next association(s) can be set up before the current one is torn down. In the United States, it is planned for the track hand off to initiate address passing and set up of new associations.

On the G/G side, the ATN provides a robust networking capability that provides self-healing capabilities as well as used to transport A/G and G/G data seamlessly anywhere in the network. It can accept standard G/G interfaces e.g., copper, fiber, or fixed RF. It operates much the same as the Internet. The Aeronautical Message Handling Service provides for the translation and transportation of AFTN message traffic using X.400 protocols. The ATS Interfacility Data Communications is used to facilitate international coordination between ground ATC automation.

3.2.1.1 ATN Security Services and Requirements

The QoS requirements for ATN are maintained by various protocols running on the ATN Upper Layers. Data Integrity is maintained by end-to-end checksums. The Transport Protocol maintains a checksum on all messages. However, this may not prove to be sufficient to meet the security requirement in some specs and application end-to-end checks may be required.

The transport protocol is primarily responsible for ensuring against mis-delivery and for ensuring receipt of messages. It also reports non-delivery should a transport connection

fail. However, it can only report the probability that mis-delivery has occurred. This is a vulnerability within the transport layer that could be exploited to gain access to messages unless upper layer protocols are used to gain additional security.

The IDRP protocol used in the ATN for exchange of routing information provides type 1 and type 2 authentications, as mentioned in the ATN SARPS subsection V. Support of type 2 authentication enables the routing information base to be protected from attackers that try to modify routing information while in transit, or which attempt to masquerade as genuine ATN Routers.

Subsection VIII of the ATN SARPS has details on some of the security services available to protect the information on the ATN. Most of these will be implemented by the ATN upper layer protocols:

- Access control methods to prevent unauthorized use of ATN resource
- Use of symmetric and asymmetric cryptographic mechanisms to provide strong authentication services
- Data Integrity services to ensure that the ATN data is not altered.

There are no requirements for confidentiality of data or the encryption of data on the ATN.

In addition, the ATN also supports a Public Key Infrastructure (PKI) services and use of X.509 certificates that are stored in a Certificate Authority (CA) Server.

Since the ATN depends on the upper layers for enhanced security, applications are often modified to make them more secure. A good example that the ATN is working on is the Protected Mode CPDLC (PM-CPDLC). It's a modified version of the original CPDLC application and is used where air/ground application demand stronger proof against mis-delivery and provide message Integrity (by using an Application Message Integrity Check).

3.3 Communication Architecture Summary

The present architecture is composed of proprietary UAV and AVCS components that communicate over largely unprotected spectrum using free text messaging for Pilot to UAV ATC communications, command and control and flight termination. Payload

communication is also unique. All three of these functions may be bundled and transit a common RF path. In today's NAS, UAV pilot to controller ATC Voice communications will most likely use the command and control path to the aircraft on the pilot side cross link to the UHF/VHF path on the ATC side. All pre-flight and post flight closeout activities will use procedures, applications and communications paths that exist today (e.g., DUATS, SAMS, Flight Service).

4 Security Assessment and Mitigation Suggestions

The following section provides a security assessment with mitigation suggestions of the following areas:

- Air-to-ground and ground-to-ground communication infrastructure
- Possible concerns and attendant mitigation activities
- Assessment of protocol suites and their potential security holes
- Assessment of ATN and IP protocols for maturity of design

4.1 Security holes in Air-to-Ground and Ground-to-Ground Infrastructure

4.1.1 Identify Security Holes in A/G infrastructure

The following section will provide a security assessment of the envisioned communication infrastructure for the Air-to-Ground communications.

4.1.1.1 Communication between AVCS and UAV (C^2 and Payload)

Interviews and online research suggest that currently the C^2 link as well as the downlink are not encrypted. Compression techniques, based on a custom sequence, are used for some of the communications. Spread spectrum and frequency hopping have been identified as either being used or planned for use to some extent (not fully identified, partially due to proprietary and confidential reasons). Even with compression techniques, spread spectrum, and frequency hopping though, the payload message can be intercepted and decoded. There is also no authentication being used. Since there is no authentication, the communication can be manipulated (modification of data or taking over control of the C^2 link). There is no identified non-repudiation. Without non-repudiation available, receipt (verified acknowledgments) of transition activities will not be possible. Non-repudiation is important in after action of events.

Security is paramount for the link between the AVCS and UAV. Frequency hopping and spread spectrum provide a good means for combating the layer 1 (Physical) denial of service attacks. Cryptographic technology can be used for encrypting the data channel (layer 2 or layer 3). Depending on the type of cryptographic technology, there may be authentication included (IPSec includes authentication). An authentication server is needed to capture the transactions for non-repudiation.

It is important to make sure that the latest in encryption algorithms are employed as well.

Earlier encryption methods such as DES are now known to have flaws. AES is the current widely deployed encryption algorithm that provides most security by enabling use of keys as big as 256 bits (DES used 56-bit to 128-bit keys).

One of the concerns with implementing this technology for UAV to AVCS communication is the hand-off process. If there is a disruption in the link during the handoff (a hard handoff vs a soft handoff) there is a chance that any established IPsec tunnel can break. If this is the case, the tunnel would have to be setup again and the system could become vulnerable at that point where an attacker might try to break into the data connection. To mediate handoff risks, there must be a "make before break" strategy, where the next pilot takes over before the last pilot ceases operations.

Another concern has to do with how IP addresses are going to be used within the UAVs. This should be a topic for further research since no information is available right now. The concern has to do with how the IP addresses are going to be assigned to the UAV. If the IP addresses are hard-coded into the UAVs, and the UAV gets handed over to another AVCS, that AVCS might be in a different IP subnet. For the UAV to keep communicating, it would have to utilize the mobile IP technology in order to keep communicating with the same IP address. There are security issues identified with using mobile IP that would have to be taken into consideration.

Key management and exchange between pilot, UAV, FAA, and any other entity needs to be established. Though this is common for the DoD environment, it is not very common for the FAA or civilian environment. Introduction of a key management structure into the FAA and the civilian environment may have obstacles.

Finally, if the UAV's plan to use multicasting to broadcast the payload data to be shared by several AVCSs, then IPsec cannot be used directly with multicast traffic, mainly due to the fact that key management is difficult with the way multicast protocol works. A workaround to this problem would be to create a GRE tunnel or something similar to tunnel the multicast traffic through or use layer 2 encryption devices at either end to perform the encryption of frames in the data link layer. This solution can be used for securing all the data paths involved with UAV communications but it is not scalable as two encryption boxes are need to support each peer-to-peer connection and as it would not scale for multiple peer-to-peer connections that are envisioned.

4.1.2 Identify Security Holes in G/G infrastructure

The following section will provide a security assessment of the envisioned communication infrastructure for the Ground-to-Ground communications.

4.1.2.1 UAV Pilot-to-Pilot Handoff

When UAVs need to be handed off from one Pilot to another, there needs to be a series of steps accomplished. It is assumed that this Pilot-to-Pilot handoff will be between two locations, and that these locations may be on the ground or in the air. In order for the handoff of control from one pilot to another to occur successfully, control must be maintained during the handoff. The only way to accomplish the task of maintaining control is to ensure the there is a "make before break" strategy. This strategy is performed by both pilots having control of the UAV at the same time, with one being the primary, and the other being the standby. In order for a pilot to gain control of the UAV, there must be a link between the two pilot locations, to pass the necessary authentication information.

Since the existing communication architecture is not yet defined, we have assumed that the pilot-to-pilot architecture will be by a communication link using IP. It is further assumed that this IP link will be deployed without the necessary protection needed on the link, similar to what the pilot to UAV currently has. This is an issue since this communication connection needs to be protected and the information needs to be authenticated.

The easiest way to secure a network is to avoid connections to external networks such as the Internet. If connections to external networks are necessary, they should be protected with firewalls to filter ingress and egress traffic. Strict firewall rule sets should be employed to make sure that only authorized hosts or systems initiate traffic or respond to communications requests. If the AVCS facilities are connected using leased communications (not shared with other users), it adds a certain level of security. However, these connections can be further made more secure by establishing encrypted tunnels between the sites. These can be implemented on the routing equipment that is responsible for forwarding packets between all points on the network.

In situations where the AVCS is a mobile unit, it's not clear what methods are used to communicate with other AVCSs. If the RF technology is used to connect the mobile AVCS to the main AVCS network, security at the Network layer must be maintained.

Since this medium is physically accessible to anyone with a transmitter/receiver, all communications using RF technology needs to be encrypted.

As with any network, it is critical to make sure that all networking equipment is properly configured with security in mind. All unneeded services running on the networking equipment should be turned off. These may include HTTP, FTP, TFTP, etc. Networking equipment running these types of services are more vulnerable to an attack. An attacker can use the 'open' TCP or UDP ports used by the services mentioned above to gain access to the device.

If SNMP is used to remotely manage the networking equipment, then only read access should be allowed. SNMP protocol has a number of known vulnerabilities and the code running on the networking equipment should be upgraded to include the latest patches that have been release by the vendors that addressee these vulnerabilities. In addition, SNMP Version 3 is the recommended version of the protocol to be used as it has the ability to encrypt the 'password' or the community string that is required by the device to respond to an SNMP request.

It is also important to use secure routing protocols within the network. The routing protocol are responsible for discovering neighbors and building the routing tables so that packets can be accurately routed to their destinations. Earlier routing protocols such as RIP have known vulnerabilities and are not scalable. RIP does not have built in authentication and hence will use information in RIP packets without verifying it. Hence an attacker could forge a RIP packet and cause all traffic to be sent to that attacker's machine. Routing protocols such as OSPF are more scalable and can be configured to authenticate the neighbors before accepting routing updates from them. Also external routing protocols such as BGP also have authentication schemes and should be used when exchanging routes with external networks or users.

4.2 Possible concerns and attendant mitigation activities

The following section discusses the attendant mitigation activities. These activities include items not specifically related to the communication security of the UAV system, but necessary for inclusion in the complete security assessment of the UAV system.

FAA Spectrum Management is concerned about protected RF service volumes command and control, payload, and flight termination when the UAV operates outside the MOA to

avoid unintentional jamming. The UAV communications should request spectrum specifically allocated for UAVs, such as the MLS band to mitigate the current issues relating to the open frequency ranges being used.

FAA Flight Standards and Aircraft Certification have system and detailed concerns. These concerns include:

- unintentional and intentional failures of the RF paths
- unintentional and intentional errors in command and control and flight termination data communications
- systems interactions on board the aircraft,
- A/G for ATC and command and control
- ground control interaction with the human operator
- appropriate pilot to controller procedures

The current FAA voice switching systems will not support phone line access for pilot-controller voice. We have assumed that the airship will act as the "bent pipe" allowing for the pilot to talk to the ATC controller via the airship.

None of the UAVs are built and operated to 14CFR21 and 14CFR91 rules. Without compliance to these rules, the FAA cannot certify and operationally approve the aircraft and the associated communications. Therefore, no matter how good the communication portion of the UAV is, the ultimate goal of routine NAS usage will not be allowed by the FAA.

Physical security of the UAV pilot location(s) needs to be part of any security assessment. The infrastructure needs to be protected and there needs to be policies and procedures established for those within the facility.

Physical security of the UAV needs to be identified. Protection of the airship during non-flight needs be maintained to ensure when the airship becomes airborne all expectations are realized. The alternative to protection of the airship on the ground, is thorough inspection of the entire airship and its systems before each flight by a team of inspectors.

Software updates and virus protection strategies need to be identified. It is possible that an airship will need to receive a critical software update while in flight. Any software update creates numerous risks. A wireless software update with an airship flying in the

NAS creates additional risks and concerns. It is recommended that software updates be performed on the ground, except when there are updates that can't wait for a landing.

Human factors need to be included in the security assessment. If the pilot is not competent or properly trained to operate the airship, then this needs to be identified.

If the UAV is a stealth aircraft it must be visible to the ATC system to assure safe separation of aircraft.

4.3 Assessment of protocol suites and their potential security holes

This section assesses each TCP/IP and the OSI (ATN) protocol suites for potential security holes as they apply to possible use for UAVs and proposes standard mitigations.

4.3.1 Vulnerabilities with the TCP/IP protocol stack

The TCP/IP protocol as it exists today was not designed with security in mind. It lacks the basic mechanisms for security such as encryption and authentication. The lack of built-in security has led to the discovery of a number of security flaws in the protocol suite that can be used to carry out a number of attacks such as sequence number spoofing, routing attacks, source address spoofing, and authentication attacks. The vulnerabilities discussed here are for IPv4. IPv6 has corrected most of the vulnerabilities but has limited implementation in the field today (discussed further in section 4.4).

IP is a best-effort, connectionless routing protocol. Transmission Control Protocol (TCP) that runs on top of the IP protocol provides a connection-oriented service between the source and the destination and brings in some reliability and guarantee of service to the TCP/IP protocol suite. However, a number of flaws have been discovered in TCP's various mechanisms such as sequence numbers, acknowledgements, 3-way handshakes, and timers. In this study we will not go into details of the operations of the TCP layer but identify the various kinds of attacks that are known.

The TCP "SYN" attacks takes advantage of how the 3-way handshake is implemented in some hosts. Before two hosts start communicating, a SYN request is sent. When a host receives a SYN request, it partially opens up a connection in the listen queue for a short amount of time until the sender replies to the SYN response (SYN+ACK). During this time, an attacker can send multiple SYN requests and never reply to the SYN+ACK

requests and thereby fill up the listen queue that can fill up quickly. Once the listen queue is filled up, it will not accept any more connections and hence a denial of service attack can occur.

IP spoofing is another attack where an intruder pretends to send data from an IP address that is not its own. This can be done by manually changing the source address of the packet before sending them out. Since there's no authentication built into the protocol, the destination has no way of checking who actually sent the packet and this can be used to gain unauthorized privileges. Another vulnerability in the TCP protocol enables an attacker to guess the sequence number in a TCP connection, and this can result in the attacker being able to setup a whole TCP connection.

Source routing is an option in the IP protocol that can be used with IP spoofing to gain access to a communications stream. By using source routing, you can specify the path through which the reply message should be sent. An attacker could specify a route that bypasses the real host and direct them to a location where they can be monitored. This problem can be avoided by turning off 'source-routing' in the routing equipment so that they drop packets with this option enabled.

Earlier routing protocols such as RIP do not have authentication built-in and hence can be exploited. An attacker can forge a RIP packet and begin advertising false routes. A router receiving these updates has no way to determine the validity of the routes. Routing protocols such as OSPF and BGP have authentication mechanisms that can be configured to authenticate the remote router before establishing a peer. These kinds of protocols are recommended to be used in critical data networks.

ICMP attacks have been common recently. ICMP is a protocol in the TCP/IP suite that is primarily used for troubleshooting to test connectivity and discover paths etc. Since there is no authentication built in to the ICMP message, denial of service attacks can be carried out using this protocol. Recent attacks have involved ICMP flooding where so many echo requests are sent from multiple workstations at the same time, causing a host, server or router to attend to these messages rather than process the legitimate traffic. Another form of attack is to send a carefully crafted 'ICMP unreachable' message that tells the host that the end device is no longer accessible, prompting the host to drop the connection. There are also other forms of ICMP attacks that are possible but if the routing devices and configured properly and host machines are patched with the latest

updates, these attacks can be avoided.

If SNMP is used to remotely manage the networking equipment, then only read access should be allowed. SNMP protocol has a number of known vulnerabilities and the code running on the networking equipment should be upgraded to include the latest patches that have been release by the vendors that addressee these vulnerabilities. In addition, SNMP Version 3 is the recommended version of the protocol to be used as it has the ability to encrypt the 'password' or the community string that is required by the device to respond to an SNMP request.

Firewalls are excellent tools to prevent against most of the security threats associated with the IP protocol. The packet filtering schemes employed by firewalls these days can even look the application layer to filter and drop suspicious packets.

As mentioned before, using IPsec can eliminate most of the vulnerabilities with IPv4. IPsec provides encryption and authentication and therefore makes it harder for an attacker to gain access to the actual TCP layer where it is possible to exploit the existing vulnerabilities. Authentication as well as Integrity protection mechanisms detect changes to certain parts of the IP header. IPv6 was designed with encryption and authentication in mind and helps in eliminating most of the vulnerabilities that exists with current IPv4. However, IPv6 has not yet been deployed widely enough and hasn't been used for long enough to know what vulnerabilities it may have.

4.3.1.1 IPSEC

IPsec can be built into the software at the application layer, implemented on the routing equipment, or implemented between firewall equipment at the source and the destination of the data. The main difference between IPsec for IPv4 and IPv6 is that in IPv6 the header was designed with security in mind and has fields in the header reserved for Authentication and Encryption parameters required for IPsec where as the IPv4 header generally has to be modified to include the additional header fields required for security.

In IP, keys or 'passwords' are used to encrypt and decrypt the data and these keys must be exchanged before the encryption process can start. The Internet Key Exchange (IKE) protocol is used for exchanging the keys. Currently there are two key distribution methods, namely 'shared key' and 'public key'. In the shared key environment the same key is used for encrypting and decrypting the data and hence it must be configured at

both end-points. Even though this method is simple, the problem with this method is that the keys have to be controlled without compromising the security of the key and it is also not scalable when there are several peer-to-peer connections with different keys. The 'public key' method is more scalable and more suitable for the UAV application where there will be several peer-to-peer connections. In the public key encryption, each peer creates a private key and a public key. The private key is never shared and the public key is widely made available. Contents encrypted with the public key can only be decrypted with the private key. Key management servers can be used to store all the public keys in a central location so that when two devices want to initiate a secure communication channel, they can obtain all the necessary keys from one location.

An example of how public key encryption might work in this study is that each UAV and the AVCS will have a private key and a public key. The private keys will be stored on the UAV and the computer system in the AVCS and never shared. Both their public keys will be stored in a key-server accessible by both. Once the public keys are exchanged by the UAV and the AVCS, the two systems can start a secure communication session. If this UAV gets handed over to another AVCS, for example, then a new key negotiation would take place between the UAV and the new AVCS and a new secure channel would be setup using the newly exchanged keys.

4.3.2 OSI (ATN) Security Vulnerabilities

The OSI protocol suite is not as widely used as the TCP/IP protocol suite is. One concern with the OSI protocol model is that since it's not widely used, there may be numerous vulnerabilities within the suite that have not been discovered yet.

From a study done by Eurocontrol, it was found that the following threats exists to the ATN, including ATN management and application services:

- Air-to-ground and ground-to-ground Air Traffic Control Messages are vulnerable to modification, reply, masquerade and jamming.
- The X.400 Message Handling System (MHS) is vulnerable to modification and masquerade.
- The OSI systems management is vulnerable to modification, replay, masquerade, and unauthorized modification of management information base.
- For applications on ATN, vulnerabilities exists that could result in Denial of Service attacks.

The vulnerabilities posted above pose a significant threat to the ATN, and hence require specific counter-measures to be implemented as soon as possible.

As a result of this work, it is believed that application messages need to be protected by "digital signatures" providing both authentication of the sender and a high quality data integrity check. Furthermore, the source of routing information needs also to be similarly authenticated.

In addition, subsection V of the ATN SARPS states that there are no security mechanisms provided in the ATN Internet layer for protecting ATN data link applications. Version 3 standards specifies an ATN information security framework, which includes:

- framework standards,
- the framework for public key infrastructure,
- the framework for provision of security services in ATN systems,
- the framework for provision of security services within the Upper Layer Communication Service,
- the framework for provision of security services within the Context Management application,
- the framework for provision of security services within other ATN applications,
- the framework for provision of security services within SM Managers,
- the framework for provision of security services within ATN Directory Servers,
- the framework for provision of security services for auditing of ATN systems,
- the framework for provision of security services for system management of ATN systems, and
- backward compatibility.

Backward compatibility may be one of the critical security risks. It is not clear whether the security function has been implemented in any working or demonstration implementations.

ATN data link applications are currently protected by upper layer security functions, if available. This is vulnerability in the ATN network layer in that it depends solely on the upper layers to secure the data. The network layers could be exploited to cause denial of service or spoofing attacks if there are no mechanisms in place to protect the network layer.

4.3.2.1 ATN transition to IP protocol suite

With IP becoming the dominant protocol suite, ICAO has recognized a need for the ATN protocol and applications suite to migrate to the IP suite. To initiate this transition ICAO has started work on converging the OSI protocol suite to operate over the IP network. This implementation is being tested for G/G communication in the South Pacific and will use the AMHS application. In the spirit of keeping everything standardized within the IETF framework the ICAO ATN Panel is working on a standard SNDCF for operation OSI over IPv4 (RFC 791) & IPv6 (RFC 2461). These will be issued in SARPS updates as well as RFCs through the IETF process.

Given that IP is the dominant protocol suite today, ICAO is beginning the process of converting from OSI to IPv6 protocols. The status of this work is:

- The ATN Panel is in the early stages of converting the ATN from an OSI based system to an IPv6 based system for ground-to-ground. SARPS validation are expected to be completed by 2006.
- Mobile IP based on IPv6 will be used as the basis for transitioning the air-to-ground part. Modifications to support Air Traffic Management A/G data communication will be standardized through the IETF RFC process, referenced, and validated in ICAO SARPS. Work is scheduled for completion by 2008.
- SARPS are to be approved at a 2008 ATN panel meeting. State approval letters to follow panel approval may take up to two years.

Since there may be OSI based ATN implementations prior to the availability of standards that have been through the state letter process, there may be some security and safety related risks to providing services over IP and OSI based applications. Also there may be

some safety and security risks that arise from a possible dual suite approach to service provisioning. It is also not clear whether the pilot or controller needs to be aware of whether they are communicating using an OSI or IP end system/application.

These risks can be addressed through design assurance and penetration testing program.

4.4 Assessment of IP and OSI (ATN) protocols for maturity of design

This section assesses IP and OSI (ATN) protocol suites for maturity of design and security. IPv4, IPv6, and OSI are the three major protocol suites (IPv4 and IPv6 as part of the TCP/IP suite and OSI as part of the OSI model suite) that are known to the communications world. These three protocol suites will be discussed below.

IPv4, which was originally developed by the Defense Advanced Research Projects Agency (DARPA) and then included with the Berkeley Software Distribution of Unix, is the most widely used network protocol today. Since it is being used on the Internet and the World Wide Web as the protocol of choice it is very mature. This protocol has been functioning on the Internet as well as within the DoD and FAA networks without any serious problems. There have been several security vulnerabilities identified with the IPv4 stack but solutions have been developed to protect its many users from them as it has matured.

IPv6 was designed to address the shortcomings of IPv4 such as security, address space, and mobile uses. There is a slow migration around the world to this protocol stack but the majority of the IP users remain on IPv4. Although there haven't been any serious security issues with IPv6 identified, this protocol stack hasn't had that much time to mature. It is a fairly new protocol, less than five years of limited use, that still needs a lot of testing and greater widespread use before declaring it a successful replacement for v4. It is expected that IPv6 will start getting more exposure in the next few years and UAV application developers should stay up-to-date with the latest developments in IPv6 if they decide to use them on the aircraft.

The OSI protocol suite was the first attempt to improve and standardize on IPv4. During the time the ATN was developed, it was the only standardized protocol stack available and it had to be implemented to make sure that ATN would be interoperable with various other ATN links. Having been tested and successfully deployed in several operational demonstrations, the ATN using the OSI protocol suite can be said to have

matured very well for the FAA's environment. It has not experienced any serious problems and does a good job with providing mobile network capability that is required in this environment. There have been various security vulnerabilities identified with this protocol as mentioned in previous sections. Most of the security features of the ATN are only available at the upper layers. Also, with IP becoming the dominant protocol suite ICAO has recognized a need for the ATN protocol and applications suite to migrate to the IP suite.

5 Concerns/Limitations/Recommendations

Based on the data gathered and analysis performed, the authors of this study offer the following concerns, limitations, and recommendations:

Concerns

- Currently there is no security, in the form of authentication and encryption, present in the pilot to UAV link.
- There's no prevention against jamming.
- No security requirements have been identified for UAV operation in the NAS
- Different UAV manufacturers implement the communications systems in their own way. No sharing of information.
- No spectrum has been identified for UAV use.
- No FAA or UAV ground communication infrastructure has been developed.
- The FAA is only beginning to assess the impact of UAV operations on the NAS.
- Assumptions need to be validated. If any of the assumptions are invalid, then those sections of the study need to be re-looked.
- Handoff from one AVCS to another AVCS should be a "make before break" communications coordination function. This will eliminate an open time when the IPSEC tunnel is broken and penetration can occur. It also provides continuous positive control of the aircraft during a handoff.
- There needs to be Handoff procedures, both between the pilot and pilot and pilot and ATC.
- There is a need to work with FAA Spectrum Management, the FCC, ICAO and ITU-T to find frequency assignments that can be uniquely assigned for UAV flight operations.
- There is a need to unbundle the three functions (C2, payload, and flight termination)

and place them on their own protected frequency or RF paths. This will eliminate a single point of failure and minimize the safety risks.

- The flight termination function should be standardized to follow 14CFR91 loss of ATC communication procedures or a return to base. This would minimize unpredictable UAV behavior upon loss of C2, ATC comm or activation of the flight termination function.
- Current phantom controller/pilots detection methods should be satisfactory in a voice environment.

6 Topics for Additional Study

During the course of this investigation many topics for further study were uncovered. Based on experience in the development of similar wireless systems, the authors believe that these topics are considered critical to the successful deployment of UAVs in the NAS.

1. A complete communication architecture study is needed to establish some standardization, where possible, in the following communication areas:
    - Command and Control (Pilot-to-Aircraft, with telemetry from aircraft-to-pilot)
    - Air Traffic Control (Pilot-to-FAA)
    - Payload (mission traffic, such as surveillance information)
    - Flight Termination (onboard or remote emergency termination)
2. Security implications need to be part of all activities from the onset, to ensure band-aids are not used after activities are completed.
3. Safety concerns need to be part of the security assessments. Safety implications need to be identified in all decisions.
4. Safety and Security assessments should be looked at for commonality to eliminate to duplication of work.
5. A clear concept of operations needs to be developed that starts with Pre-Flight and aircraft storage and end with a safe arrival and storage of the aircraft.
6. Need to perform a detailed gap analysis of the current FAA systems architecture and domestic U.S. Air Traffic Procedures and International Procedures to determine the changes required for UAVs to fly as part 91 aircraft in the NAS and internationally. An example of this is that the Access 5 Concept of Operations indicates that the pilot to controller communications

can be sent to the ATC system via leased or dial-up line. Sector phone numbers are not published, thereby eliminating dial-up lines as a means communicating with ATC. If a leased line is used to go between the pilot and the controller, there is no current NAS Voice Switch that can transition sector to sector or facility to facility. All transitions today occur by frequency assignment to the next sector or facility.

7. ATN Version 3 standards should be considered for command and control. Extensions to address CPDLC and ADS-A shortcomings could be incorporated.
8. Full System safety and security assessment, such as a SCAP needs to be performed.
9. Security processes such as key management servers, authentication, conveying a key to the aircraft, etc. in a standards based environment need to be studied and architected.

7 Conclusion

Based on the data collected, the analysis performed, the documentation and literature that was researched, and the assumptions made, the following conclusion is created.

The present architecture for the operation of UAVs consists of proprietary UAV and AVCS components that communicate over largely unprotected spectrum using free text messaging for Pilot to UAV ATC communications, command and control, and flight termination. It is imperative that security mechanisms for protection from denial of service and jamming, authentication, encryption, and non-repudiation be in place for this line of communication before UAVs can be introduced to the NAS. As a part of this report, we have also identified the importance of having flight termination capabilities as well as the need to make sure non-repudiation techniques are present for this function.

It is assumed that one way for the UAV's pilot to communicate with the FAA is by use of a "bent pipe". When the UAV pilot wants to initiate communication with ATC controllers, communication is established between the pilot and UAV and the UAV and ATC controller. Other than the risk of being eavesdropped there is no real threat to the avionics systems in the UAV with this approach, when properly designed.

ICAO currently functions using the OSI protocol stack on the ATN network. This system has been deployed for awhile and has thus had some time to mature. However, with the TCP/IP protocol stack gaining immense popularity and the need to interoperate with a growing number of new applications that only support TCP/IP, the ATN is being forced to transition towards TCP/IP. Work is currently under way for this effort and the ATN is looking at both IPv4 and IPv6, with the latter protocol having a better chance of being selected due to its attractive security features and its ability to work in a mobile environment.

It is our recommendation that if UAVs wind up embracing IP technology, vigorous security testing be done to make sure that known security vulnerabilities with IPv4 are mitigated and unknown security vulnerabilities with IPv6 are identified.

Finally, in order to deploy UAVs in the NAS, the airships must meet all FAA rules and regulations imposed by manned aircraft. A formal security assessment will need to be done on the finalized design of the UAV communication systems and airship, when this occurs.

8 Reference documents and other sources consulted

8.1 UAV Reference Documents

- The Challenges of Safely Introducing Unmanned Aircraft Systems (UAS) into the NAS (Phil Potter - UAV.ppt), AFS-430 Phil Potter 9/20/2004
- HALE ROA Access to the NAS, (Sturman Buis - UAV.ppt) Dave Buis, 8/25/2004
- UAVs… A Global Perspective, (A5EuroUVSYearbook.pdf), 9/21/2004
- HALE ROA Concept of Operations – rev 4, (CONOP_r4_2003Sept30.pdf), 9/30/2003
- HALE ROA Access to the NAS – Orientation Overview, (Access 5 OverviewOri#2CEE85.ppt), 5/18/2004
- HALE ROA Access to the NAS – Partnership to Gain ROA Access to the NAS for Civil/Commercial Applications, (Access5 Brief Oshkosh V3.ppt*)*, Oshkosh, WI, 7/2004
- Access 5 Functional Requirements Document – Rev 1, (A5_Functional_Reqmt_Doc.r1.doc), 9/5/2003
- ATN SARPS Version 3 Subsection V-22
- ATN SARPS Version 3 Subsection VIII
- Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN) II-1

8.2 FAA Documents

- FAA Air Traffic Handbook 7110.65 to assess procedural considerations.
- Federal Aviation Regulations 14CFR 21 & 91

8.3 Websites used in this study

- http://www.ja.net/CERT/Bellovin/TCP-IP_Security_Problems.html
- http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html
- http://www.computer.org/internet/v2n1/perkins.htm
- http://www.helios-is.com/atn/atnover/index.htm

8.4 Interviews

Interviews were conducted with the following groups and individuals through phone calls, emails and on site visits.

- FAA Aircraft Certification – James Sizemore & Matt Wade
- FAA Flight Standards – Phil Potter
- FAA Spectrum Management – Don Willis & Don Nellis
- FAA Voice Switch Program Manager – Bill Syptak
- FAA En Route System Planning Manager – Greg Burke
- FAA Chief Engineer –Communications – Jim Eck
- FAA Systems Engineering lead to make ICAO SARPS & IPv6 maturity assessment – Leon Sayadian.
- SAIC UAV engineers to gain insight into UAV security considerations Richard Luhr, Troy Abbott, and Bill Cronin.
- Boeing: Jed Sturman (ACCESS 5 IPT lead for infrastructure and implementation)
- UNITE Alliance – Dale Tietz

Acronyms

ACARS	Aircraft Communications Addressing and Reporting System
ADS-B	Automatic Dependent Surveillance-Broadcast
AMSS	Aeronautical Mobile Satellite Service
ASN.1	Abstract Syntax Notation One
ATIS	Automated Terminal Information Service
ATN	Aeronautical Telecommunications Network
ATC	Air Traffic Controller
AVCS	Air Vehicle Control Station
BIS	Boundary Intermediate System
C^2	Command and Control
CFR	Code of Federal Regulations
CLNP	Connectionless Network Protocol
CPDLC	Controller Pilot Data Link Communications
D-ATIS	Digital Automated Terminal Information Service
DoS	Denial of Service
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FIS	Flight Information Services
ICAO	International Civil Aviation Organization
IDRP	Inter-Domain Routing Protocol
IETF	Internet Engineering Task Force
IFR	Instrument Flight Rules
ISO	International Organization for Standardization
ITU-T	ITU Telecommunication Standardization Sector
LOS	Line of Sight
MOA	Military Operations Areas
MODE-S	Mode Select Beacon System
NAS	National Airspace System
NAT	Network Address Translation
NASA	National Aeronautics and Space Administration
NOTAMS	Notice to Airmen
OSI	Open System Interconnection

PICS	Protocol Implementation Compliance Statements
PKI	Public Key Infrastructure

PM-CPDLC	Protected Mode CPDLC
QoS	Quality of Service
RF	Radio Frequency
RFC	Request for Comments
ROA	Remotely Operated Aircraft
RSA	An Algorithm used for Encryption and Digital Signatures
RTCA	Requirements and Technical Concepts for Aviation
SARPS	Standards and Recommended Practices
SCAP	Security Certification and Authorization Package
SNDCF	Subnetwork Dependent Convergence Function
SNMP	Simple Network Management Protocol
TCAS	Traffic Alert and Collision Avoidance System
UAV	Unmanned Aerial Vehicle
VDL	VHF Data Link
UHF	Ultra High Frequency
VFR	Visual Flight Rules
VHF	Very High Frequency
VoIP	Voice over Internet Protocol